Site Recovery Manager のセキュリティ

Site Recovery Manager 8.1

vmware®

最新の技術ドキュメントは VMware の Web サイト（https://docs.vmware.com/jp/）にあります
このドキュメントに関するご意見およびご感想がある場合は、docfeedback@vmware.com までお送りください。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴイエムウェア株式会社
105-0013　東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

VMware Site Recovery Manager のセキュリティについて

『Site Recovery Manager のセキュリティ』では、Site Recovery Manager のセキュリティ機能の概要について説明します。

Site Recovery Manager 環境の保護に役立てるため、本書では Site Recovery Manager に組み込まれているセキュリティ機能と、攻撃から環境を守るためにとれる手段を説明します。

- Site Recovery Manager を適切に動作させるうえで不可欠な外部インターフェイス、ポート、およびサービス
- セキュリティに影響する構成オプションと設定
- ログファイルの場所と目的
- 必要なシステム アカウント
- 最新のセキュリティ パッチの取得に関する情報

対象者

この情報は、Site Recovery Manager のセキュリティ コンポーネントについて理解しておく必要がある、IT 意思決定者、アーキテクト、管理者などを対象としています。

本書について

1

本書を使用して、Site Recovery Manager 環境のセキュリティ機能や、攻撃から環境を守るためにとれる手段について確認してください。

- Site Recovery Manager のサービス

  Site Recovery Manager の処理は、Site Recovery Manager Server のホスト マシンで実行されるいくつかのサービスによって決まります。

- Site Recovery Manager のネットワーク ポート

  Site Recovery Manager では、クライアントや他のサーバとの通信用に、構成可能なネットワーク ポートが使用されています。Site Recovery Manager で使用されるポートが、ファイアウォールでブロックされないことを確認する必要があります。

- Site Recovery Manager の構成ファイル

  Site Recovery Manager の一部の構成ファイルには、環境のセキュリティに影響を与える可能性のある設定が含まれています。設定が適切でないと、Site Recovery Manager 環境の適切な動作に影響する場合があります。

- Site Recovery Manager の証明書およびキー

  Site Recovery Manager は、TLS 証明書とプライベート キーを使用して、ネットワーク通信を保護し、他のサーバとの認証を安全に確立します。

- Site Recovery Manager に保存されている認証情報

  Site Recovery Manager では、ストレージ レプリケーション アダプタ (SRA) および Windows レジストリのデータベースの認証情報が暗号化された形式で保存されています。

- Site Recovery Manager のライセンス ファイルおよび EULA ファイル

  Site Recovery Manager のライセンス ファイルと EULA ファイルは、Site Recovery Manager Server のホスト マシンに保存されています。

- Site Recovery Manager のログ ファイル

  Site Recovery Manager は、動作情報をログ ファイルに記録します。ログ ファイルには、プライベート キーやパスワードなどの機密情報は含まれません。

- Site Recovery Manager のアカウント

  Site Recovery Manager はシングル サインオン (SSO) を使用して、vCenter Server および Platform Services Controller にアクセスします。

- Site Recovery Manager のセキュリティ アップデートおよびパッチ

  VMware から提供されている、Site Recovery Manager のセキュリティ アップデートとパッチを適用できます。また、ホスト オペレーティング システムのベンダーが提供する、ホスト オペレーティング システムのセキュリティ アップデートとパッチも適用できます。

- Site Recovery Manager Server のセキュリティ強化に関するベスト プラクティス

  Site Recovery Manager Server のセキュリティを強化するためのベスト プラクティスにより、発生する可能性のあるセキュリティの問題から環境を保護することができます。

Site Recovery Manager のサービス

Site Recovery Manager の処理は、Site Recovery Manager Server のホスト マシンで実行されるいくつかのサービスによって決まります。

表 1-1. Site Recovery Manager に必要なサービス

サービス名	起動時間	説明
VMware vCenter Site Recovery Manager Server	自動	Site Recovery Manager のコア機能を提供します。
VMware vCenter Site Recovery Manager 組み込みデータベース	自動（組み込みデータベースを使用する場合）	Site Recovery Manager 組み込みデータベース用の vPostgres サーバです。
VMware vCenter Site Recovery Manager クライアント	自動	VMware vCenter Site Recovery Manager クライアント（Tomcat、HTML5 ユーザー インターフェイス）の機能を提供します。
サーバ	自動	ネットワーク経由のファイル共有をサポートする Windows サービスです。
Workstation	自動	リモート サーバへの接続を作成して維持する Windows サービスです。
保護ストレージ	自動	機密データを格納する Windows サービスです。

Site Recovery Manager のネットワーク ポート

Site Recovery Manager では、クライアントや他のサーバとの通信用に、構成可能なネットワーク ポートが使用されています。Site Recovery Manager で使用されるポートが、ファイアウォールでブロックされないことを確認する必要があります。

Site Recovery Manager Server は、1 つのネットワーク ポートですべての受信トラフィックを受け取ります。デフォルト ポートは 9086 です。組み込みデータベースを使用するように Site Recovery Manager を構成すると、Site Recovery Manager の組み込みデータベースは、ローカルホストのネットワーク トラフィックをローカルのループバック インターフェイスで受け取ります。デフォルト ポートは 5678 です。

デフォルト ポートがブロックされる場合や、他のアプリケーションで使用される場合は、インストール プロセスの間に、Site Recovery Manager 用に別のポートや組み込みデータベースのトラフィックを選択できます。受信ポートのトラフィックを有効にするように、ネットワーク ポリシーを構成する必要があります。インストール後に変更できるポートの詳細については、『Site Recovery Manager のインストールおよび構成』ドキュメントの「Site Recovery Manager Server インストールの変更」のトピックを参照してください。

Site Recovery Manager Server は、ローカル サイトにある Platform Services Controller、vCenter Server、ESXi の各ホストやアレイと通信します。ネットワークのファイアウォール ポリシーで、ローカル サイトにあるすべてのコンポーネントのネットワーク ポートへのトラフィックが有効になっていることを確認する必要があります。すべての VMware 製品が使用するデフォルト ポートのリストについては、http://kb.vmware.com/kb/1012382 を参照してください。

Site Recovery Manager ペアのローカル サイトとリモート サイト間の接続は、VPN のようなプライベートな接続にする必要があります。ローカルの Site Recovery Manager Server は、リモート サイトにある Site Recovery Manager Server、Platform Services Controller、および vCenter Server と通信し、ネットワーク プロバイダは、トラフィックを有効にするため、適切なネットワーク ポリシーを確保する必要があります。

Site Recovery Manager 用に開いておく必要のあるすべてのポートのリストについては、『Site Recovery Manager のインストールおよび構成』ドキュメントの「Site Recovery Manager 用のネットワーク ポート」のトピックを参照してください。

Site Recovery Manager の構成ファイル

Site Recovery Manager の一部の構成ファイルには、環境のセキュリティに影響を与える可能性のある設定が含まれています。設定が適切でないと、Site Recovery Manager 環境の適切な動作に影響する場合があります。

表 1-2. Site Recovery Manager の構成ファイル

ファイルまたはディレクトリの場所	説明
`<installation_folder>\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml`	Site Recovery Manager Server のシステム構成を定義します。 注　この構成ファイルは、移動または削除しないでください。 Site Recovery Manager ユーザー インターフェイスの [サイト ペア] タブの [詳細設定] を使用して、Site Recovery Manager インスタンスのシステム設定を安全に変更できます。
`<installation_folder>\VMware\VMware vCenter Site Recovery Manager Embedded Database\bin\vmw_vpg_config\`	組み込みのデータベース構成ファイルが含まれます。 注　この構成ファイルは、変更、移動、または削除しないでください。
`<installation_folder>\VMware\VMware vCenter Site Recovery Manager\config\extension.xml`	Site Recovery Manager Server の拡張機能の構成を定義します。`extension.xml` ファイルには、デフォルトのユーザー ロールとその権限の定義が含まれます。 注　この構成ファイルは、変更、移動、または削除しないでください。
`C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.properties`	Site Recovery Manager HTML5 ユーザー インターフェイスの構成を定義します。 注　この構成ファイルは、移動または削除しないでください。 <phonehomeEnabled> の値を true から false または false から true に変更することによって、Site Recovery Manager HTML5 ユーザー インターフェイスのテレメトリ設定を安全に変更することができます。

Site Recovery Manager の証明書およびキー

Site Recovery Manager は、TLS 証明書とプライベート キーを使用して、ネットワーク通信を保護し、他のサーバとの認証を安全に確立します。

CA 証明書/プライベート キー（またはその両方）	場所および説明
TLS 証明書と Site Recovery Manager Server エンドポイントのキー	Windows 証明書ストアの `Certificates\vmware-dr\Personal\Certificates` フォルダにあります。 インストールの際にカスタム証明書を指定しなかった場合は、Site Recovery Manager が証明書を生成します。
TLS 証明書と、Site Recovery Manager のインストール中に作成された `solution` ユーザー用キー	Windows 証明書ストアの `Certificates\vmware-dr\su-<Site Recovery Manager UUID>\Certificates` フォルダにあります。
TLS 証明書と、リモート サイトの `solution` ユーザー用キー	Windows 証明書ストアの `Certificates\vmware-dr\remote-su-<Site Recovery Manager UUID>\Certificates` フォルダにあります。 Site Recovery Manager は、ペアリング プロセス中にファイルを作成します。
TLS 証明書と、Site Recovery Manager のインストール中に作成された HTML5 ユーザー インターフェイスの `solution` ユーザー用キー	`C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib\h5dr.keystore` ファイル内。
TLS 証明書と Tomcat サーバ エンドポイント用キー	`C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf\h5dr-server.keystore` ファイル内。 TLS 証明書と Site Recovery Manager Server エンドポイント用キーと同じです。
Site Recovery Manager Server の CA 証明書と、TLS 証明書	`<installation_folder>\VMware\VMware vCenter Site Recovery Manager\bin\<SRM_Server_IP_address><ca>.p7b` ファイル。 インストールの際にカスタム証明書を指定しなかった場合は、Site Recovery Manager が証明書を生成します。 証明書をクライアントのトラスト キーストアにインポートして、ユーザーが Site Recovery Manager Server 証明書を暗黙的に信頼するようにできます。

注　Site Recovery Manager インスタンスを保護するために、プライベート キーの情報の抽出や共有は行わないでください。

Site Recovery Manager の認証メカニズムの詳細については、『Site Recovery Manager のインストールおよび構成』ガイドの「Site Recovery Manager の認証」トピックを参照してください。

Site Recovery Manager に保存されている認証情報

Site Recovery Manager では、ストレージ レプリケーション アダプタ (SRA) および Windows レジストリのデータベースの認証情報が暗号化された形式で保存されています。

管理者グループのメンバーであれば、認証情報にアクセスできます。

レジストリ パス	説明
HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\db:<datastore name>	<datastore name> システム データストアを使用して、Site Recovery Manager データベースにアクセスするための認証情報。
HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\Vmware DR\Creds\storage-arraymanager <manager id>-username	<manager id> で識別されるアレイ マネージャに接続する際に、SRA で使用する必要があるユーザー名。
HKEY_LOCAL_MACHINE\System\CurrentControlSet\services\ Vmware DR\Creds\storage-arraymanager-<manager id>-password	<manager id> で識別されるアレイ マネージャに接続する際に、SRA で使用する必要があるパスワード。

Java キーストア **h5dr.keystore** の認証情報は、**C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\lib** フォルダにある **h5dr.properties** ファイルに保存されています。Java キーストア **h5dr-server.keystore** の認証情報は、**C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-client\conf** フォルダにある **server.xml** ファイルに保存されています。

Site Recovery Manager のライセンス ファイルおよび EULA ファイル

Site Recovery Manager のライセンス ファイルと EULA ファイルは、Site Recovery Manager Server のホスト マシンに保存されています。

表 1-3. Site Recovery Manager のライセンス ファイルおよび EULA ファイル

ファイルまたはディレクトリ	説明
<installation_folder>\VMware\VMware vCenter Site Recovery Manager\en\	Site Recovery Manager のエンドユーザー使用許諾契約書ファイルが格納されたディレクトリ。
<installation_folder>\VMware\VMware vCenter Site Recovery Manager\en\open_source_license.txt	Site Recovery Manager のオープン ソース ライセンス ファイル。
<installation_folder>\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\EULA-en.rtf	Site Recovery Manager の組み込みデータベースのエンドユーザー使用許諾契約書ファイル。
<installation_folder>\VMware\VMware vCenter Site Recovery Manager Embedded Database\share\open_source_license.txt	Site Recovery Manager の組み込みデータベースのオープン ソース ライセンス ファイル。

Site Recovery Manager のログ ファイル

Site Recovery Manager は、動作情報をログ ファイルに記録します。ログ ファイルには、プライベート キーやパスワードなどの機密情報は含まれません。

Site Recovery Manager Server のログ

Site Recovery Manager は、システム ログ ファイルを `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\Logs` ディレクトリに保存します。Site Recovery Manager Server からの最新のメッセージが `vmware-dr-<number>.log` ファイルに記録されます。

Site Recovery Manager Server を再起動した場合や、現在のログ ファイルがファイル サイズの上限を超過すると、Site Recovery Manager は現在のログ ファイルをアーカイブし、新しいログ ファイルを作成します。

ログ ファイルのディレクトリを変更するには、`<installation_directory>\VMware\VMware vCenter Site Recovery Manager\config\vmware-dr.xml` 構成ファイルのディレクトリの XML 要素に、カスタムのディレクトリ名を入力します。また、`vmware-dr.xml` ファイルの logLevel XML 要素を更新することで、各コンポーネントのログ レベルを変更することもできます。デフォルト レベルは、すべてのコンポーネントで詳細になっています。

重要　アクセス制御リストを構成して、ログ ファイルへのアクセスを制限します。

表 1-4. ログ レベル

レベル	説明
エラー	エラーのログ エントリのみを表示します。
情報	情報、エラー、および警告のログ エントリを表示します。
最詳細	情報、エラー、警告、詳細、および最詳細のログ エントリを表示します。
詳細	情報、エラー、警告、および詳細のログ エントリを表示します。
警告	警告とエラーのログ エントリを表示します。

Site Recovery Manager は次のようなコンポーネントをサポートしています。

- Default
- Replication
- Recovery
- ストレージ
- StorageProvider
- Vdb
- Persistence

`vmware-dr-<number>.log` ファイルには、リモート側との認証プロセスや接続に関するセキュリティ メッセージが含まれていません。

Site Recovery ユーザー インターフェイスのログ

Site Recovery Manager は、Site Recovery ユーザー インターフェイスのログ ファイルを `C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm-clients\logs` ディレクトリに保存します。最新のメッセージは、`dr.log` ファイル内に記録されます。

`C:\ProgramData\VMware\VMware vCenter Site Recovery Manager\runtime\srm client\webapps\dr\WEB INF\classes` ディレクトリにある `log4j.xml` ファイルのレベル値要素を更新することで、各コンポーネントのログ レベルを変更できます。デフォルト レベルは、すべてのコンポーネントで情報になっています。

表 1-5. ログ レベル

レベル	説明
エラー	エラーのログ エントリのみを表示します。
警告	警告とエラーのログ エントリを表示します。
情報	情報、エラー、および警告のログ エントリを表示します。
デバッグ	デバッグ、情報、エラー、および警告のログ エントリを表示します。
トレース	最も詳細な情報を表示します。

Site Recovery ユーザー インターフェイスで使用される tomcat サーバは、次のようなコンポーネントをサポートしています。

- HTTP 非同期 I/O
- ハンドラ呼び出し時間ごと
- vCenter Server L10N カタログ
- SRM
- VR
- 共通

Site Recovery Manager のアカウント

Site Recovery Manager はシングル サインオン (SSO) を使用して、vCenter Server および Platform Services Controller にアクセスします。

ユーザー アカウント

デフォルト構成では、vCenter Server 管理者には Site Recovery Manager に対する管理アクセス権があります。インストール後 Site Recovery Manager へのログインを初めて試行するときに、管理者の認証情報を使用する必要があります。

管理者の認証情報を使用すると、他のユーザーが vSphere Web Client を使用して Site Recovery Manager にアクセスすることを許可できます。

Site Recovery Manager のロール、特権、および権限の詳細については、『Site Recovery Manager 管理』ドキュメントの「Site Recovery Manager の特権、ロール、および権限」を参照してください。

Solution ユーザー アカウント

Site Recovery Manager は、インストールの際に **solution** ユーザーを作成して、vCenter Server との認証に使用します。**solution** ユーザーは、各 Site Recovery Manager インスタンスに固有で、Site Recovery Manager、vCenter Server、および Platform Services Controller で内部的に使用されます。

Site Recovery Manager は、拡張リンク モードを使用しないサイトのペアリング プロセスの間に、各リモート サイトに、追加の **solution** ユーザーを作成します。Site Recovery Manager は、**solution** ユーザーを使用して、リモート サイト上で必要な処理を実行します。

Site Recovery Manager は、インストールの際に HTML5 ユーザー インターフェイスに対して **solution** ユーザーを作成し、vCenter Server との認証中に HTML5 ユーザー インターフェイスで使用します。ソリューション ユーザーは、各 Site Recovery Manager インスタンスに固有で、Site Recovery Manager HTML5 ユーザー インターフェイス クライアント、vCenter Server、および Platform Services Controller で内部的に使用されます。

注 **solution** ユーザー アカウントに関連付けられているロールや特権を削除したり、変更したりしないでください。

solution ユーザーと、ローカル サイトとリモート サイト間の認証の関する詳細については、『Site Recovery Manager のインストールおよび構成』ドキュメントの「Site Recovery Manager の認証」トピックを参照してください。

Site Recovery Manager のセキュリティ アップデートおよびパッチ

VMware から提供されている、Site Recovery Manager のセキュリティ アップデートとパッチを適用できます。また、ホスト オペレーティング システムのベンダーが提供する、ホスト オペレーティング システムのセキュリティ アップデートとパッチも適用できます。

Site Recovery Manager ホスト オペレーティング システムのバージョン

Site Recovery Manager Server でサポートされるホスト オペレーティング システムの詳細については、https://docs.vmware.com/jp/Site-Recovery-Manager/8.1/rn/srm-compat-matrix-8-1.html にある『Site Recovery Manager 8.1 互換性マトリックス』を参照してください。

Site Recovery Manager のパッチおよびセキュリティ アップデートの適用

Site Recovery Manager のセキュリティ パッチとセキュリティ アップデートは、既存の Site Recovery Manager インストールのインプレース アップグレードを実行することによって適用します。Site Recovery Manager のアップグレードの詳細については、『Site Recovery Manager のインストールおよび構成』の「Site Recovery Manager Server のインプレース アップグレード」トピックを参照してください。

Site Recovery Manager Server のセキュリティ強化に関するベスト プラクティス

Site Recovery Manager Server のセキュリティを強化するためのベスト プラクティスにより、発生する可能性のあるセキュリティの問題から環境を保護することができます。

Site Recovery Manager のセキュアな操作は、Site Recovery Manager Server オペレーティング システムの適切な構成と保守に依存します。

- Site Recovery Manager は、サポートされているホスト オペレーティング システム、データベース、およびハードウェアでのみ実行します。Site Recovery Manager が、サポートされているホスト オペレーティング システムで実行されていないと、Site Recovery Manager が正しく実行されない場合があります。
- オペレーティング システムの最新のアップデートとパッチを適用して、悪意のある攻撃からホスト オペレーティング システムを保護します。Site Recovery Manager の最新のアップデートとパッチを適用して、Site Recovery Manager に関する既知の問題に対処します。
- Site Recovery Manager を仮想マシンとして実行する場合、Site Recovery Manager のデプロイ環境の整合性を確認します。『vSphere セキュリティ』ドキュメントの「仮想マシンのセキュリティのベスト プラクティス」のトピックを参照してください。
- ソフトウェアのインストールを限定的に行い、Site Recovery Manager で使用しないサービスを無効にすることで、リソースを解放し、サーバへの攻撃の可能性を軽減します。不要なソフトウェアやサービスは、CPU、ストレージ、メモリ、および帯域幅のリソースを浪費し、サーバに対する攻撃の可能性を高めます。
- サーバ アクセスを管理者のみに限定します。攻撃者が利用可能なアカウントの数を制限するため、サーバにアクセスできるアカウントの数を制限します。
- Site Recovery Manager が使用するネットワーク ポートを確認し、ファイアウォールを構成してサーバを保護します。